CLAIMS:

We claim:

1. A method for classifying electronic mail message transfer requests for policy enforcement comprising the steps of:

identifying a source of an incoming electronic message;

classifying said source; and,

applying a message transfer policy associated with said classification for said source.

2. The method of claim 1, wherein said identifying step comprises the step of identifying a network address for said source.

3. The method of claim 1, wherein said classifying step comprises the step of classifying said source as one of a trusted source, a blocked source, and a suspect source.

4. The method of claim 1, wherein said classifying step comprises the step of classifying said source as one of an authenticated source, a trusted source, a blocked source, an anonymous source, and a suspect source.

5. The method of claim 3, wherein said classifying step further comprises the step of classifying said source as a blocked source where said source appears in a realtime black hole list.

6. The method of claim 3, wherein said classifying step further comprises the step of classifying said source as a suspect source where said source appears in a realtime black hole list.

7. The method of claim 4, wherein said classifying step further comprises the step of classifying said source as an authenticated source only where an authenticated connection has been established with said source.

8. The method of claim 3, wherein said applying step comprises the step of limiting transfer of messages from a source classified as suspect.

9. The method of claim 4, wherein said applying step comprises the step of limiting transfer of messages from a source classified as anonymous.

10. A system for classifying electronic mail message transfer requests for policy enforcement comprising:

a mail server;

a set of mail transfer policies, each policy having an association with a corresponding source classification;

at least one table of source identities having a particular classification; and,

a classifier coupled to said mail server and said at least one table.

11. The system of claim 10, wherein said at least one table comprises at least one table selected from the group consisting of a table of trusted sources, a table of authenticated sources, a table of suspect sources, a table of blocked sources, and a realtime black hole list.

12. A machine readable storage having stored thereon a computer program for classifying electronic mail message transfer requests for policy enforcement, the computer program comprising a routine set of instructions which when executed by a machine cause the machine to perform the steps of:

identifying a source of an incoming electronic message;

classifying said source; and,

applying a message transfer policy associated with said classification for said source.

13. The machine readable storage of claim 12, wherein said identifying step comprises the step of identifying a network address for said source.

14. The machine readable storage of claim 12, wherein said classifying step comprises the step of classifying said source as one of a trusted source, a blocked source, and a suspect source.

15. The machine readable storage of claim 12, wherein said classifying step comprises the step of classifying said source as one of an authenticated source, a trusted source, a blocked source, an anonymous source, and a suspect source.

16. The machine readable storage of claim 14, wherein said classifying step further comprises the step of classifying said source as a blocked source where said source appears in a realtime black hole list.

17. The machine readable storage of claim 14, wherein said classifying step further comprises the step of classifying said source as a suspect source where said source appears in a realtime black hole list.

18. The machine readable storage of claim 15, wherein said classifying step further comprises the step of classifying said source as an authenticated source only where an authenticated connection has been established with said source.

19. The machine readable storage of claim 14, wherein said applying step comprises the step of limiting transfer of messages from a source classified as suspect.

20. The machine readable storage of claim 15, wherein said applying step comprises the step of limiting transfer of messages from a source classified as anonymous.